


# أمن المعلومات

## GS224-11



### الأدلة الرقمية أمن المعلومات

## 1 - الجرائم المعلوماتية

في عصرنا الحاضر، تعددت أشكال جرائم المعلوماتية وأنواعها وتغيرت، لدرجة أنه يطلق عليها عدّة مسميات في الوقت نفسه. فهناك من يستخدم لفظ «الجريمة الإلكترونية»، وآخر يستخدم لفظ «جرائم الإنترنت»، وثالث يستخدم «جرائم الحاسب الآلي أو الحاسوب»، ورابع يمزج بين اثنين أو أكثر من ذلك. ومهما تعددت المسميات فإنه يمكننا القول إنه لا يمكن أن تتم جريمة معلوماتية إلا بوجود قصور أو تراخٍ في أنظمة أمن المعلومات، أو بتجاوز تلك الأنظمة بطرق غير شرعية، وعليه فإنّ هناك علاقة وطيدة بين أمن المعلومات وجرائم المعلوماتية. فأمن المعلومات يشكّل الدرع الواقي من تلك الجرائم، وهذه الجرائم تحاول اختراق ذلك الدرع وهناك صراع دائم بين الطرفين.

يعرّف مكتب التقييم الأمريكي جريمة الحاسب الآلي بأنها: «الجريمة التي يؤدي فيها الحاسب الآلي دوراً رئيساً». ويُعدّ هذا التعريف تعريفاً عاماً شاملاً لشريحة كبيرة جداً من الجرائم لدرجة أنه يمكن أن يشمل بعض الجرائم التقليدية.

## 1 - الجرائم المعلوماتية

- الجريمة ذات العلاقة بالحاسب الآلي (Computer Crimes).
  - إساءة استخدام الحاسب الآلي (Computer Abuse).
  - التحايل باستخدام الحاسب الآلي (Computer Fraud).
  - الوصول غير المرخص (Unauthorized Access of Computer Systems).
- مما سبق يمكن تعريف الجريمة المعلوماتية بأنها: «كل عمل ينتج عنه ضرر متعمد يستخدم الحاسب الآلي وتقنية المعلومات لإلحاق الضرر بالمعلومات أو أجهزتها أو مستخدميها».

من أهداف جرائم المعلوماتية ما يلي:

- التخريب وتدمير الأجهزة والبيانات.
- تعطيل الخدمة.
- تحقيق أرباح مادية.
- التجسس بأنواعه.
- إبراز المهارة والعبث من قبل الهواة.

## 2 - خصائص الجرائم المعلوماتية

1

الصعوبة في كشفها: وتعني الصعوبة في اكتشاف أن هناك جريمة وقعت، بغض النظر عن مرتكبيها. فقد تقع جرائم معلوماتية معينة ولا يشعر أحد بأن هناك جريمة وقعت إلا بعد مرور وقت طويل، وربما لا تكتشف نهائياً، والسبب في ذلك يعود إلى أن جرائم المعلوماتية عادةً تقع في بيئة افتراضية غير ملموسة في غالب الأحيان، ولا يمكن استشعارها بشكل مادي محسوس.

2

صعوبة إثباتها: وتعني الصعوبة في إثبات وقوع الجريمة بعد اكتشافها، أو بعبارة أخرى: الصعوبة في إثبات التنفيذ. فبعد اكتشاف الجريمة والعلم بوقوعها، هناك صعوبة في إثبات أحداثها، والسبب في ذلك هو أن هذا النوع من الجرائم غالباً ما يتم تنفيذه بطرق المركزية صعبة ومهارات تخصصية عالية، ويتم في الوقت نفسه إخفاء أو مسح أي آثار قد يتركها الجاني.

## 2 - خصائص الجرائم المعلوماتية

3

الصعوبة في تحديد مرتكبيها: وتعني الصعوبة في تحديد الشخص أو الجهة التي ارتكبت الجريمة. فبعد اكتشاف وقوع الجريمة وبعد التثبت من أنها نفذت بالفعل، هناك صعوبة في تحديد الشخص أو الجهة التي نفذت، والسبب في ذلك هو أن جرائم المعلوماتية غالباً ما تُنفذ بطرق احترافية لا يوجد فيها روابط (واضحة) تربط الأحداث بمن نفذ هذه الأحداث. ويطلق بعضهم على جرائم المعلوماتية «جرائم ذوي الياقات البيضاء»؛ لأنه قد يرتكبها أناس مؤهلون تأهيلاً عالياً، وربما يحملون درجات علمية متقدمة تبعد الشكوك عنهم، ولا تدلّ مظاهرهم على أنهم مجرمون، وهذا ما يصعب عملية الربط بين هؤلاء الأشخاص والجرائم التي يرتكبونها، حتى لو كان الدافع من وراء ذلك هو إبراز المهارة وممارسة الهواية فقط.

## 2 - خصائص الجرائم المعلوماتية

4

لا تحتاج إلى أدوات وأنشطة غير مألوفة: كل ما يحتاج إليه مرتكب جرائم المعلوماتية في غالب الأحيان هو جهاز حاسب آلي واتصال بشبكة الإنترنت. فلا تجده يحتاج إلى أدوات تثير الاهتمام - كالسلاح مثلاً - بل يمكنه أن يرتكب الجريمة وهو يعمل على جهازه، كما لو كان يؤدي عملاً من الأعمال العادية، وأيضاً لا يحتاج إلى القيام بأنشطة تثير الشكوك - كالتخفي وراء سواتر، أو لبس اللثام مثلاً - بل يمكنه أن يرتكب الجريمة وهو في أحسن هيئة وأجمل مظهر.

5

سرعة التنفيذ ودقته: تعتمد جرائم المعلوماتية على أجهزة وبرمجيات تقنية المعلومات، التي هي بطبيعتها سريعة في أدائها ودقيقة في تنفيذها. لذلك تتصف هذه النوعية من الجرائم بإصابتها لأهدافها المحددة بدقة بالغة، وأنها تبدأ وتنتهي بشكل سريع.

## 2 - خصائص الجرائم المعلوماتية

6

لا تتأثر بعاملي الزمان والمكان: يطلق بعضهم على جرائم المعلوماتية «الجرائم العابرة للحدود» فيمكن ارتكاب الجريمة من أي مكان في العالم، بل من الممكن أن تكون الضحية في بلد أو قارة، والجاني في بلد أو قارة آخرين، وكذلك، يمكن ارتكاب جريمة المعلوماتية في أي وقت من ليل أو نهار، بل يمكن برمجة الجريمة، بحيث لا تقع إلا في أوقات محددة، بعد أن يتمكن الجاني من الاختفاء ومسح الآثار. وبناءً على ذلك، فإن هذا النوع من الجرائم لا يتأثر بعاملي الزمان والمكان، ويستطيع الجاني التغلب على القيود الناتجة عن هذين العاملين، وهذا بدوره يشكل عائقاً كبيراً في كشف مرتكبي هذا النوع من الجرائم وتحديدهم وإثباتها عليهم، خاصة في ظل اختلاف القوانين والتشريعات من بلد إلى آخر، فما يمكن عدّه جريمة معلوماتية في بلد قد لا يكون جريمة في بلد آخر.

## 3 - الأدلة الرقمية

ويعرّف علم التحقيق الجنائي للحاسب الآلي (Computer Forensics) بأنه: «العلم الذي يبحث في استخراج الشواهد أو القرائن الرقمية (الإلكترونية) وحفظها وتوثيقها، سواء أكانت توجد في وسائط تخزين المعلومات أو منقولة عبر شبكات المعلومات» وهو علم يشابه بدرجة كبيرة علم الطب الشرعي من ناحية فحص جهاز الحاسب الآلي ومعرفة حالته ومحتواه، ومن ثم استخراج القرائن والدلائل الموجودة فيه.

### 3 - الأدلة الرقمية

مفهوم «الأدلة الرقمية» (Digital Evidences)

يمكن تعريفها بأنها: "القرائن والشواهد التي توجد على شكل معلومات مخزنة أو منقولة في شكل رقمي (إلكتروني)" وتكون طبيعة هذه المعلومات أنها معلومات إثباتية يمكن من خلالها الاستدلال أو التأكد من قيام المستخدم بعمل ما، ومن الأمثلة على ذلك إنشاء ملف في تاريخ معين، به معلومات مهمة تخص القضية أو الجريمة، أو إرسال بريد إلكتروني، أو وجود صور فوتوغرافية رقمية، أو مخرجات نظام المعلومات الجغرافية ونظام تحديد المواقع، أو سجلات الأقفال الإلكترونية، أو مقاطع الصوت والفيديو الرقمية، وعادة ما يتم الحاسب الآلي ومحتوياته

### 3 - الأدلة الرقمية : الخصائص

قد يكون هناك دليل رقمي على شكل ملف نصي صغير الحجم، يمكن تخزينه على ذاكرة قلمية صغيرة، لكن عدد صفحاته يتعدى الألف صفحة. فالدليل الرقمي قد يكون كبير الحجم، وقد يكون معقدًا، وكذلك هو بطبيعته معرض للتدمير والتعديل بسهولة، وعلى الجانب الآخر، قد يكون الدليل الرقمي معبرًا ويصف الحال أو الحدث بدقة ووضوح، بل قد يصل في بعض الأحيان إلى أن يكون جزءًا منه هو تاريخ ووقت حدوثه.

### 3 - الأدلة الرقمية : الخصائص

- الموثوقية (Authentic): لم يعبث به، وهو فعلاً ما تم الحصول عليه دون زيادة ولا نقص، وأنه هو الدليل الرقمي المعني لا غيره. ومثال ذلك أن يكون الدليل الرقمي عبارة عن رسالة بريد إلكتروني، وتعني الموثوقية في هذه الحالة أن هذا البريد هو البريد الخاص بالقضية محل التحقيق نفسه لا غيره، وأنه يعود للشخص المعني نفسه لا غيره.
- الدقة (Accurate): دقيق في معلوماته وما يحتويه، ويمكن وصفه بكل وضوح. ومثال ذلك أن يكون الدليل الرقمي ملفاً نصياً (وثيقة) يحتوي معلومات عن خطة تنفيذ الجريمة، وتعني الدقة في هذه الحالة أن معلومات الخطة واضحة ودقيقة ولا يوجد فيها غموض.

### 3 - الأدلة الرقمية : الخصائص

- شامل كامل (Complete): أي لا يوجد به نواقص ولا نقاط مفقودة في موضوعه الذي يدل عليه. ومثال ذلك أن يكون الدليل الرقمي صورة كربونية (Carbon Copy - CC) لبريد إلكتروني، لكن لا يوجد عنوان المرسل إليه في خانة الصورة الكربونية من الرسالة، وبذلك يُعد دليل غير شامل.
- مقنع (Convincing): يولد القناعة التامة لدى المطلع عليه، فلا يوجد هناك تناقض أو تعارض أو أجزاء غير مفهومة. ومثال ذلك أن يكون الدليل الرقمي مقطع فيديو تم تصويره في إحدى المدن، لكن تظهر فيه مقاطع من مدينة أخرى، ومن ثم لا تكون هناك قناعة تامة بهذا الدليل.

### 3 - الأدلة الرقمية : الخصائص

- مطابق (مؤكد) (Conform) : أي مطابق للقواعد والأنظمة التي تحكم الأدلة الرقمية، التي تحدّد إمكانية عدّه دليلاً رقمياً أم لا. فالمعلومات العادية الخاصة بالمستخدم وملفات أنظمة التشغيل والبرامج التطبيقية العادية قد لا تكون أدلة رقمية.
- الاحتفاظ بخصائصه التقنية (Handle Technology Changes) : يحتفظ بخصائصه التقنية بغض النظر عن الوسط الذي خُزن عليه، أو تقدم وتغير التقنية المحيطة به. ومعنى ذلك، أنه يكون بالإمكان قراءة الدليل الرقمي والإطلاع عليه ومعرفة محتواه في أيّ وقت مستقبلاً، وليس مرتبطاً ببرامج معينة (غير قياسية) لا يمكن قراءته أو الإطلاع عليه إلا من خلالها.

### 3 - الأدلة الرقمية : الخصائص

- مقروء ومفهوم للبشر (Human Readable) : أي يكون في شكل كلمات وعبارات بلغة معروفة لدى من يطلع عليه. وبعبارة أخرى: لا يكون في شكل رقمي ثنائي (Digital) لا يقرأه ولا يفهمه إلا الآلة، أي لا يكون بلغة الآلة (Machine Language).

### 3 - الأدلة الرقمية : الحصول عليها

للحصول على الأدلة الرقمية، فإنه يلزم الاطلاع على محتويات الحاسب الآلي ومعالجة المشكلات الفنية فيها- إن وجدت- وبعد ذلك يجري فحصها وتحليلها للحصول على المعلومات التي قد تدين صاحب الجهاز أو تثبت قيامه بعمل ما. يجب اتباع طُرُق علمية مركزية صحيحة تضمن الحصول على دليل رقمي جيد، وفي وضع سليم غير متأثر بعملية الحصول نفسها، وفيما يلي نورد أهم الإجراءات التي يجب اتباعها للحصول على دليل رقمي جيد:

### 3 - الأدلة الرقمية : الحصول عليها

١. يجب توثيق كل ما يخص الدليل الرقمي، سواء أكان توثيقاً كتابياً أم إلكترونياً. كما يجب أن يكون التوثيق النهائي مطبوعاً على ورق، بحيث يشمل هذا التوثيق المعلومات الآتية:

- تاريخ التوثيق ووقته.
- اسم الموثّق واسم معالج الدليل الرقمي وجهة عمله.
- وصف تفصيلي للدليل الرقمي والوسط التخزيني (قرص صلب ، جهاز محمول ، ذاكرة قلمية ، ... إلخ) ، بحيث يشمل اسم الشركة المصنّعة والطراز (model) والرقم التسلسلي.
- وصف تفصيلي لجميع الخطوات التي جرى اتخاذها والتي ستنفّذ وتاريخ كل منها ووقتها. ويشمل ذلك أيّ عمليّات إصلاح لوسط التخزين الذي يحمل الدليل الرقمي إذا لزم الأمر، وما الذي جرى عمله؟ ولماذا؟ وكيف تم ذلك؟
- مكان تخزين (حفظ) الدليل الرقمي بعد الانتهاء منه، وتاريخ الحفظ ووقته.



### 3 - الأدلة الرقمية : الحصول عليها

٢. أخذ نسخة كاملة من الدليل الرقمي (قرص صلب ، جهاز محمول ، ذاكرة قلمية ، ... إلخ) على وسائط تخزين أخرى جديدة مُعدة للفحص دون المساس بوسط التخزين الأصلي للدليل الرقمي، و دون تشغيل الجهاز مطلقاً.
٣. التحقق من النُسخ التي أُخذت لوسائط التخزين الأصلية وأنها مطابقة تماماً للوسائط الأصلية حرفاً بحرف، ويمكن التحقق من ذلك باستخدام طريقة حساب البصمة الرقمية (Hash Value) للأقراص الأصلية والمنسوخة؛ للتأكد من تطابق هاتين القيمتين، وهناك عدّة خوارزميات لحساب البصمة الرقمية، ومن أشهرها خوارزمية (SHA-2).

### 3 - الأدلة الرقمية : الحصول عليها

٤. ينصح بشدة باستخدام وسائط تخزين جديدة سواء، كانت صلبة أو خارجية (USB Disks)، أو ليزرية لعمل نُسخ الفحص عليها. وعند استخدام وسائط سبق استخدامها فمن الأفضل عمل محو نهائي غير مسترجع (Wipe) لمحتوياتها، لضمان خلوها تماماً من أي معلومات سابقة قابلة للاسترجاع. وتجدر الإشارة إلى أن عمل التهيئة العادية (Format) قد لا يكون كافياً لمسح جميع المحتويات السابقة، وتُعدُّ عملية المحو النهائي غير المسترجع (Wipe) هي أنسب الطرق وأقواها في هذه الحالة.

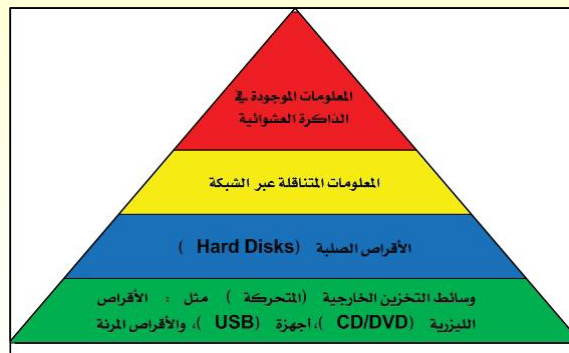
### 3 - الأدلة الرقمية : الحصول عليها

5. يجب المحافظة على سلامة الدليل الرقمي وتكامله (Digital Evidence Integrity)؛ لضمان بقاءه على حالته التي وُجد عليها دون أيّ تعديل أو زيادة أو نقص. ويمكن عمل ذلك بحساب البصمة الرقمية (Hash Value) للدليل الرقمي عند الحصول عليه مباشرة لاستخدام هذه القيمة مستقبلاً، لإثبات أن الدليل بقي على حالته التي وُجد عليها، وذلك بإعادة حساب هذه القيمة كلما دعت الحاجة إلى ذلك، وإثبات أنها مطابقة للقيمة الأولى تماماً.
6. تحليل وسائط التخزين المُعدّة للفحص باستخدام أجهزة أخرى (غالباً ما تكون مخصصة لهذا الغرض)، والاحتفاظ بالوسائط الأصلية والجهاز الأصلي على ما هي عليه، خاصة من ناحية تواريخ إنشائها أو آخر تعديل أجري عليها.

### 3 - الأدلة الرقمية : الحصول عليها

يمكن الحصول على الأدلة الرقمية من عدة مصادر، بعضها قابل للتغيير أو الفقد، ويجب التعامل معه والحصول عليه فوراً، وبعضها ثابت يمكن الحصول عليه في أيّ وقت بسهولة. وتتراوح حالة الدليل الرقمي من كونه قابلاً للتغيير أو الفقد إلى الثبات بحسب نوع الدليل الرقمي ومكان وجوده. فالأدلة الرقمية التي توجد في جهاز حاسب آلي يعمل (شغال) ويتم عرضها على الشاشة، فإنها تكون مخزنة في الذاكرة العشوائية (RAM) وستفقد فوراً إذا أطفئ الجهاز. أمّا الأدلة التي توجد على قرص تخزين صلب أو ليزري، فهي أدلة ثابتة غير قابلة للفقد الفوري، ويمكن الحصول عليها ومعالجتها لاحقاً. يوضح الشكل التوزيع الهرمي للأدلة الرقمية، من حيث ثباتها وقابليتها للفقد، حسب مكان وجودها. فالأدلة الرقمية في أسفل الهرم هي أدلة ثابتة وكثيرة العدد، كالأدلة المخزنة على الأقراص المدمجة (Compact Disk-CD)، وأقراص الفيديو الرقمية (Digital Video Disk-DVD)، بينما الأدلة في أعلى الهرم هي أدلة قليلة العدد وقابلة للفقد الفوري، كمخرجات البرامج وصفحات الإنترنت المعروضة على شاشة الحاسب الآلي أثناء تشغيله، التي عادة ما تكون مخزنة على الذاكرة العشوائية (RAM) وستفقد عند إطفاء الجهاز أو فصل التيار الكهربائي عنه.

### 3 - الأدلة الرقمية : الحصول عليها



### 3 - الأدلة الرقمية : الحصول عليها

بغض النظر عن مكان وجود الدليل الرقمي في أي مستوى من الهرم وحالته، من حيث قابليته للفقد أو الثبات، فإنه يُعدُّ دليلاً رقمياً مهماً طالما جرى الحصول عليه بحالته التي وُجِدَ عليها، ومن أهم مصادر الأدلة الرقمية ما يلي:

- البريد الإلكتروني والروابط الإلكترونية.
- الصور بشتى أنواعها.
- الوثائق وملفات النصوص بشتى أنواعها، ومنها على سبيل المثال لا الحصر: ملفات معالج الكلمات (الخطابات) (كملفات برنامج الوورد)، وملفات الجداول الإلكترونية (كملفات برنامج إكسل)، وملفات العروض التقديمية (كملفات برنامج البوربوينت)، وملفات (pdf)، والملفات النصية (txt)، وملفات الصور، وملفات الفيديو، وملفات الصوت.
- الخرائط الرقمية ومخرجات أنظمة المعلومات الجغرافية لتحديد المواقع.

### 3 - الأدلة الرقمية : الحصول عليها

- مقاطع الصوت والفيديو الرقمية.
- جداول البيانات.
- سجلات الدردشة.
- قوائم الاتصال.
- البرامج المنسوخة بطريقة غير شرعية، أو غيرها من مواد محفوظة الحقوق.
- الملفات المؤقتة (Temp Files) وملفات الكوكي (Cookie Files) .

### 3 - الأدلة الرقمية : الحصول عليها

- الملفات المحذوفة، وهنا لا بدّ من استخدام برمجيات استعادة الملفات المحذوفة، سواءً التي تأتي ضمن حزمة برامج التحقيق الرقمي أو البرامج المستقلة. وهذه الملفات يجب أن تشكل أهمية بالغة للمحقق والمحلل، لأنه عادة ما تُحذف الملفات التي تحتوي شواهد أو دلائل على الحدث أو الجريمة من قبل الجاني. وتجدر الإشارة إلى أنّه قد لا يمكن استعادة الملفات المحذوفة حتى باستخدام برمجيات الاستعادة أو برمجيات التحقيق الرقمي، وذلك إذا كُتب عليها من قبل نظام التشغيل (على أماكن تخزين هذه الملفات على قرص التخزين) وعادة ما يحصل ذلك للملفات المحذوفة منذ وقت طويل.
- ملفات التسجيل والمتابعة (Log Files) .